REMARKS

Reconsideration of this Application is respectfully requested. In response to the Office Action mailed February 24, 2005, Applicant has amended claims 8-10, 20 and 22, cancelled claims 7 and 19 without prejudice to or disclaimer of the subject matter therein, and added claim 25. Claims 1-6, 8-18, and 20-25 are pending.

Based on the above Amendment and the following Remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 112

On page 2, the Action rejects claims 7-10 under 35 U.S.C. § 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Actions states that the phrase "sufficiently large" in claim 7 is a relative term which renders the claim indefinite.

Claim 7 has been cancelled and therefore the rejection is moot.

Claims 8-10 have been amended to depend from claim 3. Since claims 8-10 do not recite the phrase "sufficiently large," they do not include a relative term rendering the claims indefinite. Therefore, Applicant respectfully requests that the rejection of claims 8-10 be withdrawn.

Rejections under 35 U.S.C. § 102

On page 3, the Action rejects claim 19 under 35 U.S.C. § 102(b) as being anticipated by Fischer. Accordingly, Claim 19 has been cancelled and therefore the rejection of claim 19 is moot.

Rejections under 35 U.S.C. § 103

On pages 4-8, the Action rejects claims 1-18 and 20-24 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,001,752 to Fischer (hereinafter "Fischer"), in view of U.S. Patent No. 6,466,048 to Goodman (hereinafter "Goodman"), in further view of the Handbook of Applied Cryptography by Menezes et al. (hereinafter "Menezes"). Applicant respectfully disagrees.

Applicant respectfully traverses the rejection as the Action fails to establish a *prima facie* case of obviousness. In order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. M.P.E.P. § 2143.

(A) For at least the following reasons, the Action does not establish a *prima facie* case of obviousness in view of the combined teachings of Fischer, Goodman, and Menezes to render claim 1 obvious.

Claim 1 recites: "A method for securing timestamping of digital data comprising the steps of: providing a **secure encryption key**; and, providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the **secure encryption key** is used for encryption operations and for test operations and in a second mode in which the **secure encryption key** is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key" (emphasis added).

Fischer, Goodman, and Menezes do not teach or suggest the claimed combination of (1) "providing a **secure encryption key**" and (2) "the processor operable in a first mode wherein the **secure encryption key** is used for encryption operations and for test operations and in a second mode in which the **secure encryption key** is only used for timestamping operations," as recited in claim 1. More specifically, the combined teachings of Fischer, Goodman, and Menezes do not teach or suggest a "secure encryption key" that is used in **both** a first mode "for encryption operations" and in a second mode "for timestamping operations."

On page 4, the Action relies on Fischer for a teaching of "a processor for performing time stamping operations with a secure encryption key," and correctly admits that "Fischer fails to disclose the system having two separate modes." As discussed below, Fischer only discloses a processor operating in a single mode that uses a private key in timestamping.

In FIGs. 1-2, Fischer discloses a processor 6 receiving a time stamp value (V1) from a clock module 4, an input value (V2) from a PC 14, a random value (V3) from a random value generator 10, and a private key from a secret private key store 8 (see Fischer col. 3, lines 13-25, col. 4, lines 35-46). The processor 6 places V1, V2, and V3 into a 64 byte word, exponentiates the 64 byte word with the private key, and stores the results as a notarized time stamp S (see Fischer, FIG. 6, col. 6, lines 9-57). Thus, the processor 6 of Fischer uses a private key received from the secret private key store 8 in a single mode to generate a notarized time stamp S. Fischer does not use the private key in **both** a first mode for encryption operations and in a second mode for timestamping operations.

On page 4, the Action then relies on the second and third embodiments of the system described in Goodman for a teaching of the missing claim features. However, Goodman does not teach or suggest a "secure encryption key" that can be used in **both** a first mode "for encryption operations" and in a second mode "for timestamping operations." As discussed below, Goodman uses a single key per mode of operation, and does not teach or suggest that a single key may be

used in two modes of operation. In column 6, line 34-column 7, line 63 and in FIG. 3 describing the second embodiment, Goodman discloses an integrated circuit 30 including operational circuitry 31 in electrical communication with a test circuitry 32 (see Goodman, col. 6, lines 36-38). The operational circuitry 31 includes an encryption processor 33, and a non-volatile memory circuit 34 for storing a **secure electronic key** (see Goodman, col. 6, lines 38-42). The encryption processor 33 is optionally in communication with a real time clock 35 that provides a time value in time-stamping functions of the encryption processor 33 (see Goodman, col. 6, lines 42-46).

The integrated circuit 30 is operable in two modes, but not at the same time, including a work mode and a test mode (see Goodman, col. 6, lines 55-56). In the work mode, the operation circuitry 31 performs predetermined processing operations of the integrated circuit 30 (see Goodman, col. 6, lines 56-59). Prior to entering the test mode, a memory erasing circuit 51 erases secure data that is stored in the non-volatile memory 34, which is used to store the **secure electronic key** (see Goodman, col. 7, lines 9-14, col. 6, lines 38-42).

In the test mode, the test circuitry 32 performs diagnostic functions using a **private test key** that is provided to the integrated circuit 30 from the non-volatile memory circuit 34 (see Goodman col. 7, lines 15-19). The encryption processor 33 receives the **private test key** from the non-volatile memory circuit 34 and uses the **private test key** to encrypt test data that is used for diagnostic purposes (see Goodman, col. 7, lines 19-21). During the test mode, access to the **secure electronic key** and secure data is **not available** within secure pathways of the integrated circuit 30 (see Goodman, col. 7, lines 53-55). Thus, Goodman discloses using the **private test key** in the **test mode**, and the **secure electronic key** in the **work mode**. Likewise, in the third embodiment, Goodman discloses disabling access to a secure electronic key in a first data bank 44a when the circuit 40 is in a test mode (see Goodman, col. 8, lines 4-7, 48-52). Goodman similarly restricts the keys in the first and fourth embodiments (see Goodman, col. 5, lines 35-40,

col. 9, lines 60-64). However, Goodman does not teach or suggest using the **private test key** in **both** the work mode for encryption operations and in the test mode for timestamping operations, and also does not teach or suggest using the **secure electronic key** in **both** the work mode for encryption operations and in the test mode for timestamping operations.

The Action does not rely upon Menezes for a teaching of a single key used in a first mode for encryption operations and in a second mode for timestamping operations, and in fact, Menezes does not teach or suggest any such features. Thus, Fischer, Goodman, and Menezes do not teach or suggest "providing **a secure encryption key**" and "the processor operable in a first mode wherein **the secure encryption key** is used for **encryption operations** and for test operations and in a second mode in which **the secure encryption key is only used for timestamping operations**," as recited in claim 1. Therefore, the Action does not establish a *prima facie* case of obviousness to reject claim 1 in view of the combined teachings of Fischer, Goodman, and Menezes since the applied references do not teach or suggest all of the claimed features. Applicant respectfully requests that the rejection be withdrawn.

Accordingly, claim 1 is allowable over the cited references and allowance thereof is respectfully requested.

Claims 2-6 and 8-10, which depend from claim 1, are also in condition for allowance because of their dependence on an allowable claim.

Claim 7, which also depends from claim 1, has been cancelled and therefore the rejection of the claim is moot.

(B) Claim 11 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested.

Claims 12-14, which depend from claim 11, are also in condition for allowance because of their dependence on an allowable claim.

(C) Claim 15 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested.

Claims 16-18, which depend from claim 15, are also in condition for allowance because of their dependence on an allowable claim.

(D) Claim 20 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested.

Claims 21-24, which depend from claim 20, are also in condition for allowance because of their dependence on an allowable claim.

New Claims

Independent claim 25 has been added to the Application.

Claim 25 recites a "A system comprising: a processor that processes a secure encryption key, said processor being operable in a first mode that processes the secure encryption key in encryption operations, and in a second mode that processes the secure encryption key in timestamping operations, wherein once the processor processes the secure encryption key in the second mode, the processor is precluded from processing the secure encryption key in the first mode."

Claim 25 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested.

Accordingly, claims 1-6, 8-18, and 20-25 are in condition for allowance and allowance thereof is respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

Respectfully submitted,

Date: June 24, 2005

Edward W. Yee
Registration No. 47,294
VENABLE LLP
P.O. Box 34385
Washington, D.C. 20043-9998
Telephone: (202) 344-4000
Telefax: (202) 344-8300

EWY:CMS/rle
DC2DOCS1\653305